

网络攻击技术

2020年8月23日 14:34

1. 侦查
2. 扫描
 - a. 端口扫描
 - i. 常见TCP熟知端口
 - 1) FTP: 21
 - 2) Telnet: 23
 - 3) HTTP: 80
 - 4) POP3: 110
 - 5) SMTP: 25
 - 6) Socks: 1080
 - ii. 常见UDP熟知端口
 - 1) RPC: 111
 - 2) SNMP: 161
 - 3) TFTP: 69
 - b. 漏洞扫描
3. 获取访问权限
 - a. 缓冲区溢出
 - b. SQL注入
4. 保持访问权限
5. 消除入侵痕迹
6. 拒绝服务攻击